



Bug 2449006 (CVE-2026-4424) - CVE-2026-4424 libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing

Keywords: Security

Reported: 2026-03-19 12:25 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-04-20 05:15 UTC ([History](#))

Alias: CVE-2026-4424

CC List: 0 users

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Version: unspecified

Environment:

Hardware: All

Last Closed:

OS: Linux

Embargoed:

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2449007](#) [2449008](#) [2449009](#)

Blocks:

TreeView+ [depends on](#) / [blocked](#)


Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2026:8558	0	None	None	None	2026-04-16 19:42:32 UTC
Red Hat Product Errata	RHBA-2026:8613	0	None	None	None	2026-04-16 22:25:07 UTC
Red Hat Product Errata	RHBA-2026:8614	0	None	None	None	2026-04-16 22:34:26 UTC

Red Hat Product Errata	RHBA-2026:8615	0	None	None	None	2026-04-16 22:31:04 UTC
Red Hat Product Errata	RHBA-2026:8844	0	None	None	None	2026-04-20 01:23:51 UTC
Red Hat Product Errata	RHBA-2026:8846	0	None	None	None	2026-04-20 02:06:36 UTC
Red Hat Product Errata	RHSA-2026:8492	0	None	None	None	2026-04-16 14:47:34 UTC
Red Hat Product Errata	RHSA-2026:8510	0	None	None	None	2026-04-16 16:09:58 UTC
Red Hat Product Errata	RHSA-2026:8517	0	None	None	None	2026-04-16 16:40:24 UTC
Red Hat Product Errata	RHSA-2026:8521	0	None	None	None	2026-04-16 16:43:51 UTC
Red Hat Product Errata	RHSA-2026:8534	0	None	None	None	2026-04-16 18:12:19 UTC
Red Hat Product Errata	RHSA-2026:8864	0	None	None	None	2026-04-20 02:48:45 UTC
Red Hat Product Errata	RHSA-2026:8865	0	None	None	None	2026-04-20 02:49:49 UTC
Red Hat Product Errata	RHSA-2026:8866	0	None	None	None	2026-04-20 03:55:07 UTC
Red Hat Product Errata	RHSA-2026:8867	0	None	None	None	2026-04-20 02:15:21 UTC
Red Hat Product Errata	RHSA-2026:8873	0	None	None	None	2026-04-20 03:43:24 UTC
Red Hat	RHSA-2026:8908	0	None	None	None	2026-04-20

Product Errata						05:15:53 UTC
----------------	--	--	--	--	--	--------------

OSIDB Bzimport  2026-03-19 12:25:44 UTC[Description](#)

A Heap Out-of-Bounds Read vulnerability exists in the RAR archive processing logic of the libarchive library. The issue arises from improper validation of the LZSS sliding window size after transitions between compression methods (PPMd and LZSS). Due to a mismatch between the allocated buffer size and the expected dictionary size, the `copy_from_lzss_window()` function performs out-of-bounds memory reads. This allows a specially crafted RAR archive to leak heap memory through the `archive_read_data()` API before integrity checks (CRC) are enforced. The vulnerability can be exploited remotely without authentication or user interaction in systems that automatically process archives, leading to disclosure of sensitive information.

errata-xmlrpc 2026-04-16 14:47:33 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via RHSA-2026:8492 <https://access.redhat.com/errata/RHSA-2026:8492>

errata-xmlrpc 2026-04-16 16:09:56 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:8510 <https://access.redhat.com/errata/RHSA-2026:8510>

errata-xmlrpc 2026-04-16 16:40:23 UTC

[Comment 4](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2026:8517 <https://access.redhat.com/errata/RHSA-2026:8517>

errata-xmlrpc 2026-04-16 16:43:50 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2026:8521 <https://access.redhat.com/errata/RHSA-2026:8521>

errata-xmlrpc 2026-04-16 18:12:18 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:8534 <https://access.redhat.com/errata/RHSA-2026:8534>

errata-xmlrpc 2026-04-20 02:15:20 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2026:8867 <https://access.redhat.com/errata/RHSA-2026:8867>

errata-xmlrpc 2026-04-20 02:48:44 UTC

[Comment 8](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2026:8864 <https://access.redhat.com/errata/RHSA-2026:8864>

errata-xmlrpc 2026-04-20 02:49:48 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10.0 Extended Update Support

Via RHSA-2026:8865 <https://access.redhat.com/errata/RHSA-2026:8865>

[2026:8865](#)

errata-xmlrpc 2026-04-20 03:43:23 UTC

[Comment 10](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:8873 <https://access.redhat.com/errata/RHSA-2026:8873>

errata-xmlrpc 2026-04-20 03:55:06 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:8866 <https://access.redhat.com/errata/RHSA-2026:8866>

errata-xmlrpc 2026-04-20 05:15:52 UTC

[Comment 12](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support

Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions

Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2026:8908 <https://access.redhat.com/errata/RHSA-2026:8908>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

